



Office of the City Auditor

DIAL IN SECURITY SYSTEM
PROJECT EVALUATION
DECEMBER 1992
(Report No. 9010B)

Michael L. Ashcraft
City Auditor

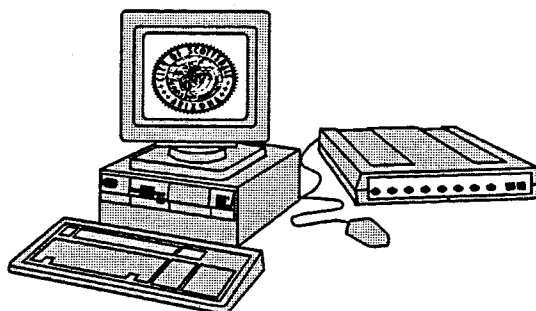
SW REF
005.8
SCOT
1992

*A
U
D
I
T

R
E
P
O
R
T*

SCOTTSDALE CITY COUNCIL

Herbert Drinkwater, Mayor
Councilman Greg Bielli
Councilman James Burke
Councilman Sam Campana
Councilman Mary Manross
Councilman Bill Soderquist
Councilman Richard Thomas



DIAL IN SECURITY SYSTEM
PROJECT EVALUATION
DECEMBER 1992
(Report No. 9010B)

TABLE OF CONTENTS

ACTION PLAN	i
EXECUTIVE SUMMARY	1
BACKGROUND	2
EXTENT AND REVIEW OF CONTROLS	6
Manual Controls	6
Automated Controls	6
IMPROVEMENTS NEEDED	8
Project Scope Not Met	8
Mandatory Requirements Not Installed	9
Redundant Power Supply: Availability	9
Redundant Power Supply: Compensation Controls	10
DISS Device Characteristics	11
Two Controls Neutralized: Password and Authorization Code	11
Dial Back	11
Log-Off for Non-Use	12
CONCLUSION	12
RECOMMENDATION(S)	13
ABBREVIATED RESPONSE(S)	13
CITY AUDITOR COMMENT(S)	14
APPENDIX A: Objective, Scope and Methodology	15
APPENDIX A1: Computer System Dial Up Security Project	
Initial Technical Specifications White Paper	19
APPENDIX A2: Dial Up Security Project Product Concurrence	
And Management Response White Paper	23
APPENDIX A3: Dial Up Access - Library Digital Equipment	
Computer System Security Variance And	
Recommendation White Paper	26
APPENDIX B: Unabridged Responses	30

DIAL-IN SECURITY SYSTEM PROJECT ACTION PLAN

No.	RELATED DISCUSSION (Page No.)	MANAGEMENT RESPONSE		IMPLEMENTATION STATUS		RECOMMENDATION (POTENTIAL FINANCIAL IMPACT SUMMARY) [PRIORITY: SEE *]
		AGREE	DISAGREE	UNDERWAY	PLANNED	
1	8, 9	X		X		Establish a centralized security function to ensure that adequate security is provided to the City's dial-in communication network and computer communication network. (Cost: \$3,000/\$5,000 Benefit: Provides control to dial-in line and the City computer network) [Priority 2]*
2	8, 9	X		X		Develop a policy and institute procedures that require the entry point (gateway) from one City computer system to another to revalidate the authenticity of the user. (Cost: nominal. Benefit: provide controls to Distributed Network) [Priority 2]*
3	9, 10	X		X		Direct the computer Security Officer to:
	11	X			X	.1) implement redundant power including automatic switch over of power source/supply when the power source for AUDITOR fails, (Cost: \$750. Benefit: enhance internal controls and better safeguard City assets) [Priority 2]*
	11	X	X		X	.2) require password changes particularly for users who are not covered by the dial back feature, (Cost: nominal. Benefit: improve computer access control) [Priority 3]*
	11, 12	X		X		.3) compel authorization code changes for dial back users, (Cost: nominal. Benefit: enhanced internal control.) [Priority 2]*
	12	X			X	.4) appraise the use of shorter (easier) passwords for users that use the dial back feature, (Cost: nominal. Benefit: customer/user satisfaction enhanced.) [Priority 3]*, and .5) require the use of automated log-off feature for non-use. (Cost: unknown. Benefit: effective use of City resources.) [Priority 3]*

- * Priority classifications:
- [1] Fraudulent practices or other serious violations are being or have been committed resulting in significant financial or equivalent non-financial losses to the City.
 - [2] The potential for incurring significant financial or equivalent non-financial losses exists, or significant revenue could be generated or recovered.
 - [3] Administration, operations, or programs can be improved; statutory non-compliance exists.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

EXECUTIVE SUMMARY

December 17, 1992

To the Most Honorable Herbert R Drinkwater, Mayor and the Members of the Scottsdale City Council:

This report summarizes the Dial-In Security System (DISS) Project and addresses steps taken by the Office of Management Systems (OMS) to evaluate, procure and implement controls on the dial-in communication network's (DICN) access to the City's computer communications network (CCN) (See Appendices A1, A2 and A3 for copies of the white papers issued as part of this project.) DICN access is used by personnel who need computer support when they are away from City facilities and is used as backup to leased lines. Unless security personnel exercise adequate oversight, computer networks that can be accessed through DICN have inherent control weaknesses. Specifically, this report discusses the additional controls that have been implemented through the installation of AUDITOR, a dial-in security device, and the areas where more stringent controls are needed: establishment of a central computer security function, upgrade of AUDITOR security features, and planning for future computer decentralized security.

A computer network that permits users to gain access via telephone service as the City's does, is available to an unlimited number of people. Even though each City computer application is afforded separate security protection, telephone access still requires special access control precautions.

Any unauthorized access to the City's DICN and CCN could result in the loss or modification of data. Additionally, confidential, proprietary or other sensitive information could be disclosed without approval. Unauthorized users could steal computer time as well as cause City staff to consume time to investigate the presence of viruses and other illegal program codes. To date, no security breaches of these types have been identified at the City.

Because our audit was instrumental in identifying DICN weaknesses and because we were involved in helping OMS management develop a Contingency Management Plan, we were asked to participate in the DISS Project. Our involvement was to participate on the evaluation team to review, evaluate and select

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

an appropriate device that would meet the security needs of the City. In addition, we evaluated the installation and implementation of OMS' selected network access control device.

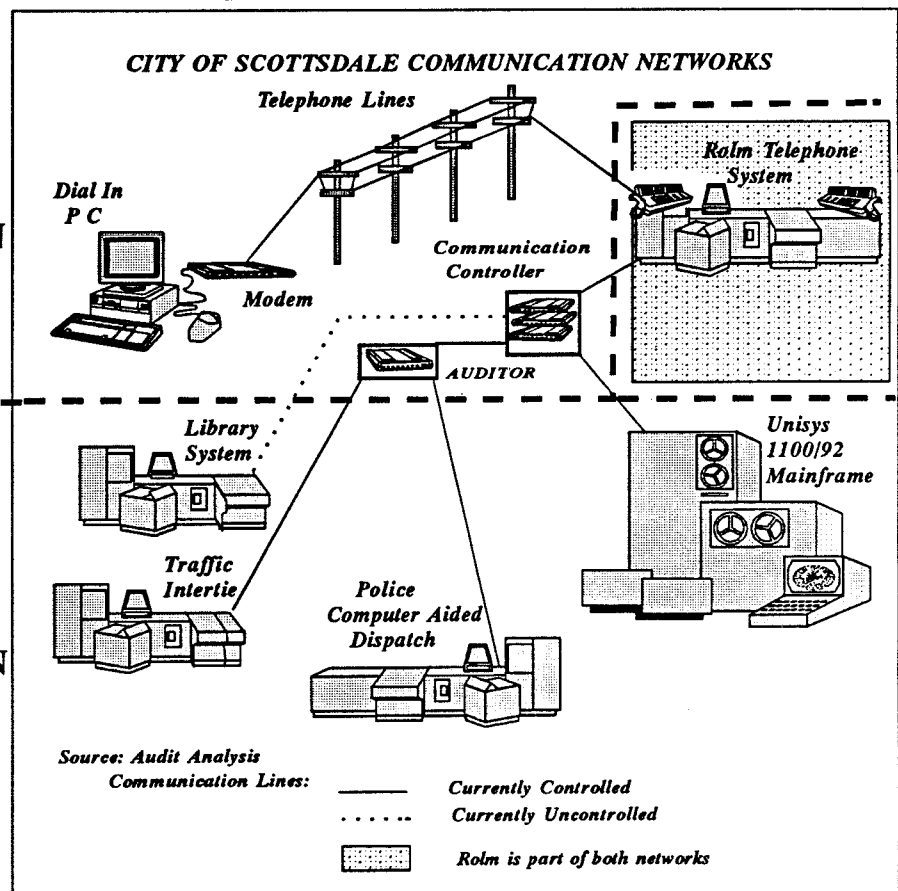
The audit was conducted in accordance with Generally Accepted Government Auditing Standards as they relate to Information Systems Auditing Standards and as required by Article III Scottsdale Revised Code §2-117 et seq. The audit was performed subject to the limitations outlined in Objectives, Scope and Methodology located in Appendix A.

BACKGROUND

The City owns and maintains one mainframe and three midrange computer systems which are housed in the Scottsdale Center for the Arts. The Unisys 1100/92 mainframe provides most of the City's automation needs, including Sperry office automation. The police use a midrange computer system, a NCR 9800, to run their Computer Aided Dispatch System. The Library employs a second midrange computer, a DEC VAX to provide an assortment of services to its customers. Lastly, City traffic lights are controlled by a third midrange computer, the Traffic Intertie System. (See Insert for a representation of Scottsdale's total Dial-In and Computer Communication Network.)

DIAL IN
COMMUNICATION
NETWORK

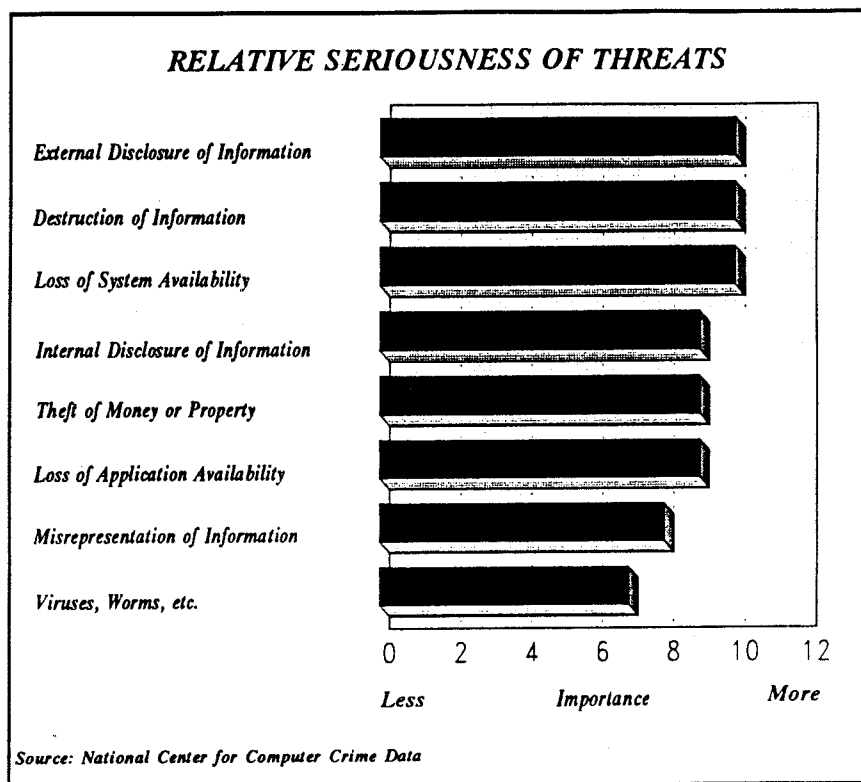
COMPUTER
COMMUNICATION
NETWORK



DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

In addition to these four systems, the City also owns and maintains a ROLM CBXII 9000 telephone system with distributed nodes (auxiliary processors). A two node telephone central processing unit is located in the Center for the Arts and a single node unit is quartered at the Corporate Yard. A stand alone telephone exchange is located at Mustang Library.

These four computer systems and the telephone system account for nearly all of the City's information management outside of the Personal Computer environment. The City provides remote data and maintenance access to the four computer and telephone systems to more than 60 staff, contract employees and elected officials. DICN access is also provided to several City computer hardware/software maintenance vendors via both local and long distance telephone lines.



Because the City's computer environment is changing, protection of this environment must constantly be enhanced. The emergence of distributed networks and the need to share data with users external to the City renders the City's information systems more accessible to unauthorized users, i.e. "hackers."

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

Although computer viruses are prolific and generate a lot of media attention, computer professionals generally have found that viruses are far less a concern than threats related to inappropriate disclosures or destruction of information (See Insert previous page).

In addition to the current DICN access to the CCN, plans include letting citizens access information via computers using dial-in communication lines. The City's Library system already grants citizen access using this method. With the Library's use of dial-in access, entry points to the DICN doubled. However, the number of possible users increased immeasurably. Since the Library began advertising their dial-in service, access to several City dial-in phone numbers specific to the Library system is no longer restricted.

Without some method of protecting DICN that restricts access, the City's dial-in telephone lines could be vulnerable to unauthorized use. If this access is obtained, protection and security is up to the individual applications available on the CCN. Each of the City's maintained systems is currently password protected. Operating systems and hardware maintained by vendors have been secured by OMS to help protect the City from identified industry-wide weaknesses (See Insert below).

COMPUTER INDUSTRY WEAKNESSES
SYSTEM MANAGEMENT AND DESIGN SAMPLES

One system in twenty yielded privilege passwords, users that are allowed to perform high level tasks, to hackers.

103 out of 150 systems had general utilities (programs that perform high level functions, i.e. erase all) on them and 88 (85%) still had the default password (original password established by the vendor) in place.

SOURCE: *Computer-Related Crimes and Auditing in the Nineties* by William H. Murray

Entry to each of the computers by maintenance personnel has been restricted since AUDITOR was installed by OMS security staff last April. Computer technicians have indepth knowledge of

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

our systems and, therefore, can present a major threat according to security professionals. These technicians are given the City's dial-in phone number to access their assigned systems and their activities must continue to be monitored closely. If security precautions are not taken, people with system access can create "back doors" or secret entrances that can become the target of hackers.

If access to computer networks is weak, any hacker has a better opportunity to break other security checkpoints and attack the data. When hackers find a weakness, they tell other hackers via electronic bulletin boards. These other hackers can then try to use the computer system.

For example, unauthorized access to the City's telephone system could result in the fraudulent use of the City's long distance lines. OMS staff realized that this type of usage would be very costly if they were not to guard against it. Consequently, OMS disabled the long distance function for any user calling into the system and then trying to dial out on a long distant line. Additionally, OMS has taken control over establishing User ID and over assigning passwords in an effort to prevent unauthorized access. These steps should help control access and protect City systems from all but the most sophisticated hackers.

A prior report, the Office of Management Systems General Controls Review (Report No. 8905, September 1990), found that DICN was not afforded protection from unauthorized access. OMS's Contingency Management Plan project also identified dial-in access as a potential security weakness. However, individual computer applications provided security protection.

Nationally, companies have reported that they have been subjected to unauthorized charges for hundreds of thousands of dollars in long distance phone bills in a single month. To prevent this type of occurrence, the City's network must continue to take security precautions.

Dial-in security systems are considered among the best deterrents against unauthorized access through dial-in telephone networks. Since security control for this mode of access was considered essential, OMS systems support instituted a project in the first quarter, 1990 to review and evaluate available dial-in network access control devices.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

**EXTENT AND REVIEW
OF CONTROLS**

The City's DISS Project was completed and the controls implemented by OMS security personnel were compared to pertinent dial-in controls. These controls can be categorized as either manual or automated.

Manual Controls

Manual controls within the security environment at the City involve the implementation of procedures and the development of automated security devices. Once a dial-in security device has been installed and protection of the dial-in lines established, procedures can provide for continued protection even if DISS' power is lost. However, daily monitoring of the transaction log for possible problems or attempted security encroachment must be performed by a security officer to help ensure the effectiveness of the control.

Automated Controls

Automated controls within the City are different characteristics or security requirements that can be implemented within DISS. The type and extent of industry recommended dial-in controls implemented by OMS are indicated below.

RECOMMENDED DIAL IN SECURITY CONTROLS

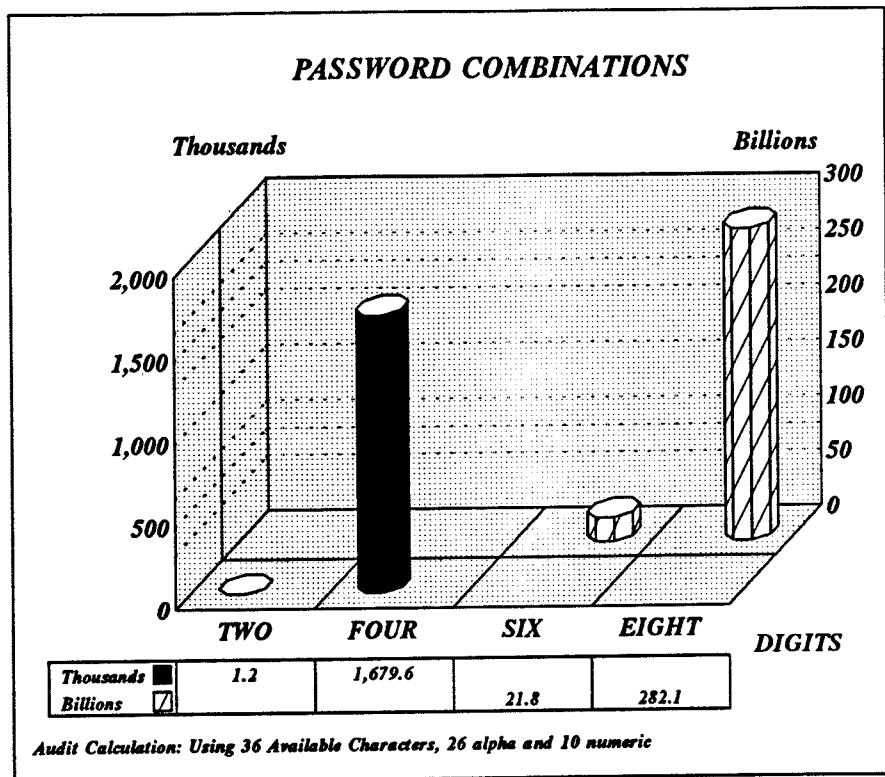
- F 1. Knowledge that a communication network has been accessed should be prevented until the caller is authenticated.*
- F 2. An authentication devise or dial back feature should be use.*
- P 3. Passwords should be used to identify users authorized to access the network.*
- F 4. Passwords should be long enough and should be non-dictionary words to discourage hackers from guessing them.*
- 5. Passwords should be changed periodically and the new password prevented from being the same password as the old one.*
- F 6. Passwords should be masked, not shown on the screen.*
- P 7. Telephone numbers used for dial in access to networks should be changed periodically and remain unlisted.*
- F 8. An authorization code should be used after dial back to verify that the number called is to an authorized user.*
- 9. Further log-on after several unsuccessful attempts should be prohibited.*
- F 10. An audit trail of all dial in activity should be produced and monitored for possible security violation attempts.*
- 11. Terminals should log-off automatically after no usage for several minutes.*
- 12. Log-on during non-business hours should be limited to specific users.*

Legend: F = Fully Implemented P = Partially Implemented

Source: Control Objectives, The EDP Auditors Foundation, Inc.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

Security controls for DICN indicate that passwords should be used and changed periodically by a security officer. These passwords should also be of sufficient length to make it almost impossible for a hacker to try all possible combinations. With the use of 36 characters, 26 alpha and 10 numeric, a one character password only provides 36 options where a 6 digit password provides in excess of 2 million possible combinations (See Insert). With the use of computers, hackers can try thousands of password options in a relatively short period of time. Consequentially, a password containing more digits is required to help block unauthorized access.



Another common security feature involves disconnecting users when terminal activity stops for a certain period of time. A security device should also hang up on the caller after the authorized user has been identified. The security device should then call the user back, at a prescribed phone number. If this call back feature is not practical, such as when a user is travelling, then an authentication device, such as a magnetic card, should be employed to confirm that the user is authorized to access the system.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

**IMPROVEMENTS
NEEDED**

Our analysis of AUDITOR determined that the security level of the City's communication network could be improved with the implementation of more stringent control features.

Project Scope Not Met

Our analysis found that the Rolm Telephone system is not protected by AUDITOR. This control omission allows any password ID of the three telephone nodes' sign-on screens to be approached without the user's authorization being confirmed. Although OMS controls Rolm system security, back doors could still exist. Knowledge of these hidden entrances could allow unauthorized access to and alteration of telephone functions, including improper use of City long distance telephone lines. This breach of security could result in the loss of thousands of dollars. OMS system support personnel encountered problems trying to get dial-in phone calls routed to AUDITOR before granting calls access to the telephone system. They determined that to remedy this would have created another problem. In turn, this would have hindered dial-in problem resolutions and maintenance by authorized personnel. OMS staff plan to research this security weakness further.

Second, dial-in access to the Library system is not fully protected. Citizen access to the library catalog information bypasses the AUDITOR, thus creating a security weakness. These Library clients all utilize the same ID and password. While this ID currently has very limited functions within the Library system, connecting the Library system to other City computer systems in the future, as planned, could produce a problem without compensating controls. We concurred with this bypass request but offered a recommendation: *The Management System Administrator should ensure the establishment of access security at entry points of the communication network. This security should be developed and monitored by a centralized security function.* (See Appendix A3 for details.)

OMS was aware that effective security measures must not only exist on the external computer side of the network, but must be similarly present where computer to computer access is provided through internal networks. OMS must continue to develop security mechanisms to ensure unauthorized users do not enter the CCN. (See Insert next page.)

No one person or function within the City is required to maintain comprehensive records of when computer systems are accessed and who has been granted authorization.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

DIAL IN

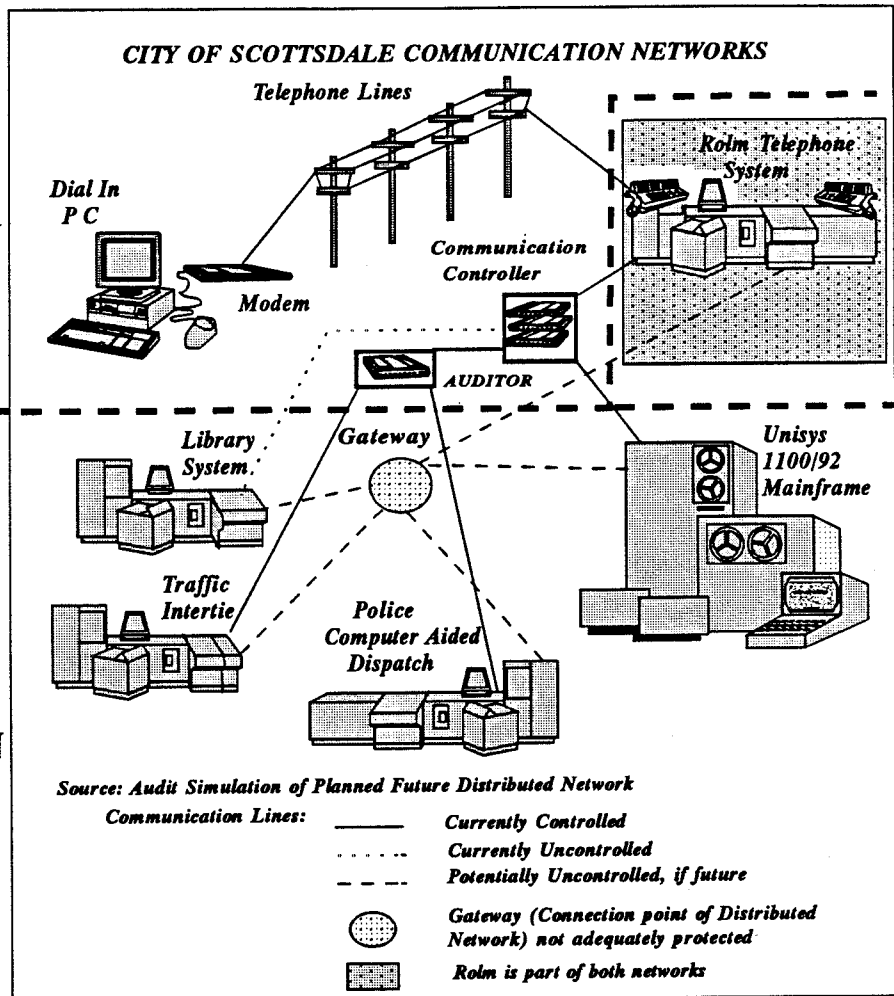
COMMUNICATION

NETWORK

COMPUTER

COMMUNICATION

NETWORK



**Mandatory Requirements
Not Installed**

We disclosed that AUDITOR was lacking adequate physical controls in two areas related to redundant power and compensating controls.

**Redundant Power Supply:
Availability**

During this review, we discovered that AUDITOR was still missing an important feature involving the availability of a redundant power supply. Redundant power is an auxiliary power unit that automatically activates when the main power supply fails. At the time of product testing, this control feature was not available, nor was it available when the City entered into the contract with the vendor. Currently, AUDITOR still does not have a redundant power supply even though the backup was promised by the vendor when the contract was signed. Without redundant power, access to DICN will not be controlled if AUDITOR loses its main power supply. In effect, this is the same as not having a security device for DICN.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

With AUDITOR disabled, any hacker with the proper equipment and knowledge of City dial-in phone numbers has unlimited access to the DICN. As a result of this finding, we would only concur with the purchase of this product with reservations. At the time, we stated, *the plan to eventually install the redundant power supply, when it is available, helps alleviate any of our long-term security concerns* (See Appendix A2 for details).

**Redundant Power Supply:
Compensation Controls**

To help ensure that we would concur with their plans, OMS management offered to install additional controls to compensate for the lack of a redundant power supply. OMS management persuaded the vendor to issue a credit of \$465, the price of a spare power supply, if the City purchased a redundant power supply for \$1,200. This power supply had a target release date of June 1991, but was delayed.

Initially, OMS planned to provide a temporary solution to the power problem. Notification of power failures were to be made through the environmental panel in the computer room. (This panel provides alarm indicators when systems fail to function as designed.) OMS management purchased a spare power supply for AUDITOR and initiated computer operator training in the event that AUDITOR's primary power system fails and needs to be replaced. Additionally, OMS indicated that they had planned on replacing the spare power unit when the vendor provided redundant power supply finally received Underwriter Laboratory approval.

OMS system support staff indicated that since the temporary solution has been in use for approximately a year without failure, since the computer operators have been trained, and since the alarm has been programmed to display on the console, the redundant power supply system was no longer needed. This "work around" as described by the OMS Administrator suited the purpose during project testing. However, the Administrator was aware of this solution's shortcomings and anticipated the purchase of a redundant power supply. City DICN is not protected when AUDITOR is without a functioning power supply. Although the time frame for uncontrolled dial-in lines could be as little as a few minutes or as long as several hours, we feel redundant power is a cost-effective solution that helps assure maximum protection.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

DISS Device Characteristics

Our review discovered that four control characteristics could be strengthened.

**Two Controls Neutralized:
Password and Authorization
Code**

OMS' Security Officer has established user passwords which are ten digits long. This control feature should provide more than satisfactory security. Second, good control involves the use of authorization codes. When AUDITOR calls an authorized user back, this code is essential before the computer will connect the user to the network.

Even though password and authorization controls were established by the Security Officer, their effectiveness will diminish over time. Passwords are not scheduled to be changed unless an employee quits. Allowing authorized users to employ the same dial-in password indefinitely provides hackers a much better chance of unveiling the password. Hackers with a phone number, password, and no dial back security features to contend with can access the DICN. Changing the authorization code periodically would enhance controls of the dial back feature.

Dial Back

Further analysis of the AUDITOR characteristics disclosed that the dial back feature is being used. Dial back is considered an excellent security control feature. Once the caller's password has been authenticated, AUDITOR hangs up and then calls the user at a preset phone number. This option provides superior security protection and helps offset the lack of changing passwords. Additionally, enough security is provided that the password need be only four digits long followed by easy to remember "fill" such as six x's.

The current 10 digit password has been criticized by some users as being unnecessarily long and difficult to remember. If familiar four digit passwords were employed, users would be less likely to write down their passwords which would make it more difficult for unauthorized users to gain access information. However, not all authorized user ID's use the dial back feature. City personnel who travel and need access to the City's computer cannot have an established preset number for AUDITOR to call back. In these cases, only a password check is performed.

Applying the previous control concern, unauthorized access to the DICN can be more easily obtained if the password is known. With access to DICN, hackers have unlimited time to attempt to

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

break application security. This fraudulent activity could be harmful to the City.

Log-Off for Non-Use

Final scrutiny of the AUDITOR characteristics uncovered that the "log off for non-use" option was not purchased. Once any user has gained access to the DICN and has ceased activity for a specific amount of time, connection with the DICN should be severed. Such a procedure helps keep lines free for other users and discourages hackers. Hackers should not be provided unlimited time to perform their craft. The more time an unauthorized user is allowed on any network, the greater the likelihood that inappropriate actions may occur.

Authorized users should also be disconnected from DICN if activity stops. There may be arguable reasons for the lack of activity, or possibly, the user just forgot to log off when he or she finished work. In any case, authorized and unauthorized users can tie-up valuable resources (dial-in lines). Allowing users to "needlessly" occupy a dial-in line impacts the productivity of other users who may need immediate access to the City's network.

CONCLUSION

Although AUDITOR, the OMS installed security device provides additional protection to the DICN to all City computer and telephone systems, several areas of concern exist. AUDITOR could provide even better controls to both DICN and CCN if security policies and controls characteristics were implemented more aggressively.

We believe that the DICN and the CCN and telephone systems should be required to enter through AUDITOR. However, the City has decided to allow dial-in access to citizens in several areas. This feature should provide adequate control but would make easy access more difficult.

Until formalized security plans have been developed for future distributed computing, a centralized security function should be established to ensure that access to both the DICN and the CCN are properly controlled. If entry is granted allowing one City computer to access another at any time then password security should be established to **revalidate user authenticity**.

DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

Additionally, DISS should aggressively restrict access to the DICN. The benefit of reducing unauthorized access is substantial while implementation costs are relatively low.

RECOMMENDATION(S)

We recommend that the Management Systems Administrator:

- 1) Establish a centralized security function to ensure that adequate security is provided to the City's dial-in communication network and computer communication network;
 - 2) develop a policy and institute procedures that require the entry point (gateway) from one City computer system to another to **revalidate the authenticity of the user.**
 - 3) Direct the computer Security Officer to:
 - 3.1) implement redundant power including automatic switch over of power source/supply when the power source for AUDITOR fails,
 - 3.2) require password changes particularly for users who are not covered by the dial back feature,
 - 3.3) compel authorization code changes for dial back users,
 - 3.4) appraise the use of shorter (easier) passwords for users that use the dial back feature,
 - 3.5) require the use of automated log-off feature for non-use.
-

**ABBREVIATED
RESPONSE(S)**

(Unabridged responses are in
Appendix B)

- 1) Management Agrees - "Any application need for dial-in access to these systems will be accomplished with placement of effective security controls."
- 2) Management Agrees - "As part of the installation of computer systems under the City's migration to 'open system,' inter-computer security will continue to be a primary implementation consideration."
- 3.1) Management Agrees - "The fully redundant power supply for the dial-in security system is now available."

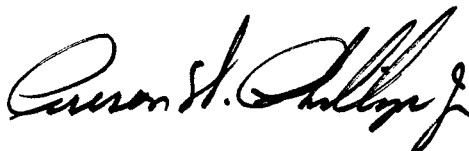
DIAL-IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

- 3.2) Management Agrees - "OMS will effect a program to change passwords on all call back bypass customers who do not have passwords already coded within a [sic] their personal computer."
- 3.3) Management Agrees - "Management agrees that forcing the two digit authorization code changes for dial back users will provide an additional level of security, but believes that implementing the feature is **not necessary** at this time."
- 3.4) Management Agrees - "The recommendation to appraise the use of shorter passwords has been completed."
- 3.5) Management Agrees - "This feature is not currently available from the dial-in security vendor."

**CITY AUDITOR
COMMENT(S)**

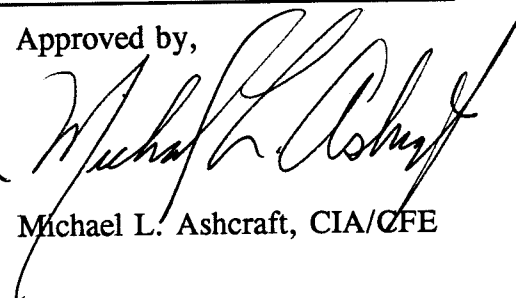
- 1) OMS's response only addresses centralized security of dial-in access. Security of distributed computers, such as the Library's, is not under the control of OMS's Software Support group.

Respectfully submitted,



Preson W. Phillips Jr., CISA

Approved by,



Michael L. Ashcraft, CIA/QFE

PP/MLA:Gail Crawford, CPS

Appendix A
Objective, Scope and Methodology

**OBJECTIVE, SCOPE,
AND METHODOLOGY**

The objectives of this assignment were to (1) guarantee the Request for Bid included all controls necessary to provide adequate security to the dial in telephone lines, (2) actively participate in product examination to help assure that the City purchased a DISS that would provide maximum security for dial in access modes to both computer and telephone systems and (3) evaluate whether the installation and implementation parameters of the selected DISS, named AUDITOR, would accomplish project objectives. Additionally, during this review, we were asked to (4) examine security considerations related to allowing dial in access at the Library that would bypass planned OMS controls.

We developed our audit program to guarantee that controls necessary to provide adequate protection to the dial in communication lines were identified. We obtained and reviewed a copy of the technical specifications draft developed by the project team. To decide if the initial security requirements in the technical specifications were sufficient as well as feasible to implement, we sought the experience of several local security professionals at Salt River Project and Valley National Bank. Both companies had installed dial back security but have had to establish compensating controls after limiting dial back use. Other security information essential to dial in communications security standards was also gathered. Comparison was made to initial technical specifications and our recommendations were submitted to the project manager for consideration. (See Computer Systems Dial Up Security Project Initial Technical Specifications White Paper Appendix A1 for details.)

To participate in the product evaluation, we worked with OMS system support personnel to test DISS. All security alternatives were tried, both "correctly" and "incorrectly" to determine if they provided the security protection promised. The main power supply for DISS was deactivated to evaluate redundant power capacities of the unit. Further, all power was turned off to test DISS protection. Our test results were presented to the project manager for consideration. We eventually concurred with the product selected by OMS management, after being assured that compensating controls would be implemented. (See Appendix A2 for details.)

We continued our evaluation to learn if the selected AUDITOR would accomplish the project's security objectives. After AUDITOR was installed and tested by OMS, we started our testing. We tried to access the computer network employing prescribed procedures. Also, using as many unauthorized techniques as we could devise, we tried to enter the network but, were unsuccessful in our attempts. Additionally, we disabled AUDITOR's power supply and tried the backup power supply. Alarm controls were also evaluated. Further, we reviewed dial in security procedures and AUDITOR's implemented security parameters. Final security concerns were discussed with OMS management.

UNAUTHORIZED TECHNIQUES

Test performed:

Incorrect phone number.
Invalid time of day.
Invalid password.
No password.
Invalid authorization code.
No authorization code.

Source: Audit Analysis

During this review, OMS asked us to examine the security risks of allowing the Library Computer Systems' dial in access to bypass OMS controls. We independently tested the operating software of the DEC computer and the Atlas software used by the Library. The Library communication network was also analyzed to ensure no connectivity existed to other City communication networks. We eventually concurred with the bypass request but with reservations. (See Appendix A3 for details.)

Our work was done between April 1990 and April 1992 in accordance with Generally Accepted Government Auditing Standards as they relate to Information Systems Auditing Standards. The Water Resource Telemetry System was not a part of this study because it is not under the control of OMS nor does dial in access to it exist. We did our test work in the OMS

DIAL IN SECURITY SYSTEM PROJECT
City Auditor Report No. 9010B

office located in the SCA building. The review of the Library system was conducted at the Civic Center Library. The Management Systems Administrator provided written comments on a draft of this report. These remarks are encompassed where appropriate and are in (Appendix B, Management Responses.)

Appendix A1
Computer System Dial Up Security Project
Initial Technical Specifications
White Paper

April 30, 1990

TO: John Krusemark, Systems Support Manager

FROM: Sonny Phillips, Senior EDP Auditor

COMPUTER SYSTEM DIAL UP SECURITY PROJECT

The efforts of the project team to provide the City with the best possible dial up security appears to be progressing steadily. With the information you have provided and some limited additional inquiry I have a few suggestions that the project team should review and consider relative to the Technical Product Specifications section of the Invitation to Bid. Potential changes relative to item number 5:

1. OBTAIN MANagements COMMITMENT ON DIAL BACK BEFORE MAKING THAT A REQUIRED OPTION. Salt River Project and Valley National Corporation, both previously using the dial back security option, have discontinued that security feature due to "access" problems. Although The City does not currently foresee any access problems, which are created mainly through the use of switchboards, future expansion of this management tool should be weighed. Salt River just discontinued the dial back feature leaving the EDP Auditors unsatisfied with the dial in security. All ports were now set up for direct dial increasing the possibility of unauthorized access. Valley National installed an additional password security feature that randomly generates a new password every 60 seconds in sync with the mainframe or security device. The dial back security option may provide the best security; however, if that feature is not installed the system may not afford the same security as another system that uses additional means of security, not relying on dial back as a security feature. By not relying on a dial back security but some more protective password feature the security system could provide a possible cost saving.

2. CHANGE MINIMUM NUMBER OF PASSWORD CHARACTERS FROM FOUR TO SIX. This increase raises the security protection by escalating the possible combinations of characters required to match the correct password. Statistically, it is virtually impossible for a hacker to try all of the possible combinations of a six digit password.

Suggested additions:

1. DISCONNECT AFTER A PRE-SET NUMBER OF ERRONEOUS ATTEMPTED ENTRIES. This security feature is a necessity on dial in lines in an effort to limit continuous attempts at breaking the password. The perpetrator would have to continuously redial in an effort to breach security. Unless the security system can determine the actual phone number where the erroneous calls are originating, it is better to prevent connections than to take the port out of service. Taking the port out of service in the current environment, would reduce the number of lines available for users who need access, thus reducing service.
2. DISCONNECT AFTER A PRE-SET AMOUNT OF TIME OF INACTIVE LINE USAGE. In the event that an authorized user does not sign off the system, they would be disconnected after some time (several minutes) of non-activity. This disconnect would help keep lines available for users who need access without increasing the number of dedicated lines necessary to provide adequate service.

If anything else regarding security or other issues affecting this project should come to my attention either before or during the pre-bid meeting, I will notify you and the project team of any suggested modifications to the specifications prior to them becoming finalized.

cc: Karen Donahue, Communications Services Manager,
Bill James, Systems Specialist
Shannon Tolle, Communication Specialist

Appendix A2
Dial Up Security Project
Product Concurrence
And
Management Response
White Paper

December 31, 1990

TO: Preson Phillips, Assistant City Auditor

FROM: Jeff Denning, Management Systems Administrator

DIAL-IN SECURITY SYSTEM

Sonny, as you know, we have completed our evaluation for the Dial-up security system and have selected Millidyne, the low bidder. I have been advised by staff that we have obtained verbal "conditional" concurrence of the Auditor's Office and would like you, via reply to this memo, to confirm same.

Staff also indicated you had concerns in respect of back-up power and that Millidyne's product, "The Auditor," did not currently have UL approval on their back-up. Millidyne expects UL approval by June 1991. Your concurrence is "conditional" based on Millidyne receiving UL approval. We have arranged temporary work around this that includes storing back-up power supplies on site.

- * Notification of power failure will be made through our environmental panel in the computer room.
- * Our computer operators will train their replacement.
- * When Millidyne is granted UL approval in 1991, we plan to forward fit our systems.

If a power failure occurs, the system will act like it is not there - all users can enter the system as they do now using the security measures currently in place. The operator can replace the failed power pack in minutes, reset the system, and the system will become functional.

Current procurement procedure does not require Council approval; the funds have been encumbered and purchase requisitions approved through senior management. Since we asked you to participate in the evaluation, we would like your concurrence before proceeding. Please indicate such concurrence by reply to this memo.

January 3, 1991

TO: Jeff Denning, Management Systems Administrator

FROM: P.W. "Sonny" Phillips, Assistant City Auditor

DIAL-IN SECURITY SYSTEM PROJECT

Jeff, we appreciated the opportunity to participate in the evaluation process of the Dial-in Security system project. As such, we will provide a written conclusion regarding the project.

Earlier we did have concerns regarding the lack of an UL approved redundant power supply for Millidyne's product "The Auditor." However, with OMS's formal plan to temporarily work around the problem by using spare parts and by establishing a notification system in case of possible product power failure, our security concerns have been reduced. Also, the plan to eventually install the redundant power supply, when it is available, helps alleviate any of our long-term security concerns.

The one concern that we still have relates to when the yet to be UL approved redundant power supply will be available. Without these pieces of equipment, the vendor does not satisfy item eight of the technical product specification portion of the request for bid.

In the best interest of the City, we feel that some type of penalty should be assessed the vendor, Millidyne, in the event the required equipment is not available by a specific date. One option would be to hold back a portion of the payment due (contracted price) until the required equipment is delivered and installed.

Except for the uncertain delivery date of the redundant power supply, I feel "The Auditor" should be able to provide adequate security over the City's dial-in access modes for both computer and telephone systems.

Appendix A3
Dial Up Access - Library Digital Equipment Computer System
Security Variance Concurrence
And
Recommendation
White Paper

May 9, 1991

TO: Linda Saferite, Library Director
Jeffrey Denning, Management Services Administrator

FROM: Michael L. Ashcraft, City Auditor
P.W. "Sonny" Phillips, Assistant City Auditor

DIAL UP ACCESS - LIBRARY DIGITAL EQUIPMENT COMPUTER SYSTEM

In February, 1991 the Library system upgrade project manager had a new Digital Equipment Computer (DEC) delivered to the City's computer room. During the initial setup, Office of Management Systems (OMS) staff discovered that the new DEC had the capability to handle 24 dial up telephone lines. Library management planned to use all 24 communication ports for dial up access to the Library catalog system (Atlas). However, they had not requested the service of the Network Access Control System (dial up security) controlled by OMS. This office was asked to evaluate the wisdom of allowing dial up access to the Library's DEC without directing calls through OMS's dial up security device.

Based on tests conducted, access controls implemented in the DEC control program and the Atlas system were found to be adequate. Ease of use by the public is the reason Library management designed dial up to use one dial up identification code (ID) and no passwords. This lack of individual ID's will complicate the tracking of possible unauthorized entrances to other operations performed by DEC. In spite of this weakness, Library management designed compensating controls to ensure adequate restrictions are afforded dial up access. When tested, the compensating controls appeared to work both effectively and efficiently.

This review was directed toward determining whether adequate and effective access controls were provided the Library's computer. Germane administrative and operational control practices that Library staff employed during the business analysis phase of the Library system upgrade project were not included in the scope of this evaluation. Security features of the DEC operating software and the Atlas system were independently tested:

DEC operating software (control program)

- Individual User ID - A unique identification code assigned each user.
- Password security - Unpublished authorization code known only to each user.
- Access restrictions - User ID only allowed certain processing functions(dial up, local, etc.).
- Restricted time slot - ID only allowed to sign on to the system specific hours of the day.
- Sign-on log - Captures all sign-ons to the system with time of day of occurrence.
- Security violations log - Seizes each unauthorized operation that is attempted.
- Restricted Crossover - Restricts user ID from entering the DEC network function that permits connectivity to other communication networks.

Atlas Catalog System

- Time limit on usage - User ID limited to specific amount of time per sign-on (20 minutes).
- Limited functions - Dial up ID is restricted to one menu that allows three operations.

While the control program has excellent individual user identification and password security, Library management chose not to engage these control features to make sure the public had easy dial up access to Atlas. Implemented controls appear to satisfactorily restrict the dial up ID to only authorized functions. Limiting processing functions and time per sign-on reduces computer usage which in turn creates operational

efficiency. Some of these regulating controls were available in the control program others developed within the Atlas system.

Access to the Unisys network from the DEC control program is currently not available. Nevertheless, plans to place computer processing in the user areas (open systems architecture) and connect these systems using a communications network should compel establishing security at the entrance (gateway) to that network.

Interviews were conducted with Digital Equipment technical personnel in an effort to understand better the DEC environment and the security features available. Also city auditors and security personnel where the Atlas Library System with dial up access has been installed were contacted to determine if any security problems had been encountered.

RECOMMENDATION:

The Management Systems Administrator should ensure the establishment of access security at entry points of the communication network. This security should be developed and monitored by a centralized security function.

A response to this recommendation is not necessary at this time. However, upon completion of audit work related to dial up security efforts, this office will request that the Management Systems Administrator respond to this and any other recommendations presented.

cc: Robert Frost, Community Services General Manager
Carder Hunt, Management Services General Manager
Audit file

Appendix B
Unabridged Responses

December 2, 1992

TO: "Sonny" Philips - Assistant City Auditor

FROM: Jeff Denning, Management Systems Administrator 

OMS RESPONSES TO AUDIT REPORT 9010B

Attached is OMS' response to the City Auditor project evaluation of a Dial In Security System installed in OMS.

The responses are consistent with what we have discussed during the past few weeks. If you need any clarification please let me know so we can respond expeditiously.

cc: Carder Hunt
John Krusemark

City of Scottsdale

Office of Management Systems

Responses to

Audit Report

Dial In Security System

Project Evaluation

Report No. 9010B

Office of Management Systems
Responses to Audit 9010B
Dial-In Security System

- 1.0 Establish a centralized security function to ensure that adequate security is provided to the City's dial-in security communication network and computer communication network.

MANAGEMENT AGREES - Centralized security is provided through the Software Support group in OMS.

The installation of the dial-in security system provides protection to all non-public access computer communication networks at the City. This device is monitored continuously by OMS Computer Operations staff.

The dial-in security system is not connected to the City's Library system. There are currently no plans for connection. The Library system has been enhanced to allow inter-Library communication and direct dial-in access by patrons. The dial-in security system works on the principle of pre-programming the User-ID, location, and expected password of the customer gaining access to the computer using dial-in access. Patrons do not have User-ID. Imposing the dial-in security system on the Library would negatively impact the Library's ability to serve their customers. As a matter of security protection, the Library will not be connected to the City's computer communication infrastructure until potential security issues have been resolved.

While local area networks are being implemented throughout the City, the controlling computer mechanisms can be placed in the customer area. Outside access is not an automatic feature in the "open systems" environment. Any application need for dial-in access to these systems will be accomplished with the placement of effective security controls.

- 2.0 Develop a policy and institute procedures that require the entry point from one City computer system to another to revalidate the authenticity of the user.

MANAGEMENT AGREES - Computer to computer security has always been a major consideration in both distributed and "open systems" computing environments. These security issues were identified in the initial evaluation of the "open systems". Such considerations, for example, led to the decision to maintain a separate communication environment for dial-in patrons to the Library system.

As part of the installation of computer systems under the City's migration to "open system", inter-computer security will continue to be a primary implementation consideration.

- 3.1 Direct the Security Officer to implement redundant power including automatic switch over of power source/supply when the power source of AUDITOR fails.

MANAGEMENT AGREES - The fully redundant power supply for the dial-in security system is now available. Installation will be completed by the end of January, 1993.

- 3.2 Direct the Security Officer to require password changes particularly for users who are not covered by the dial back feature.

MANAGEMENT AGREES - The periodic changing of passwords has proved to be an effective deterrent to unauthorized access. This is a practice encouraged by OMS for all customers having a User-ID. Changing the passwords for the dial-in security system is a function performed by the System Support group in OMS. OMS will effect a program to change passwords on all call back bypass customers who do not have passwords already coded within a their personal computers.

The dial-in security system adds another level or security to the City's computer systems. Before the dial-in security system was installed, all access required the User-ID, a four character password, and then other access authorization before being given access to various applications. The dial-in security system enhances security by requiring a 10 digit entry password, a call back feature, and an authorization code. Minimally, all dial-in customers are required to enter the 10 digit entry password. Only a few customers are granted access with call back bypass and is necessitated by the mobility of the customer. This includes OMS technical support staff and selected City staff away on business trips.

- 3.3 Direct the Security Officer to compel authorization code changes for dial back users.

MANAGEMENT AGREES - Before the implementation of the dial-in security system, computer access was granted through a User-ID and password on the computer systems. The dial-in security system provides additional security levels by requiring a separate 10 digit password, a dial back option, and a two digit authorization code. The dial back option ensures the person attempting to gain access is at a predefined location. Management agrees that forcing the two digit authorization code changes for dial back users will provide an additional level of security, but believes that implementing the feature is not necessary at this time. The feature will be reconsidered as implementation of the "open systems" results in increased activity in dial-in computer access.

- 3.4 Direct the Security Officer to appraise the use of shorter (easier) passwords for users that use the dial back feature.

MANAGEMENT AGREES - The recommendation to appraise the use of shorter passwords has been completed. Making the password easier for the customer by shortening it would also make it easier for the potential "hacker" to break the password. Staff concluded, therefore, that using shorter passwords would not be in the best interest of added security.

OMS' understanding of the issue is that longer passwords are difficult to remember. OMS recommends leaving the password at its present ten digits and working with the customers to develop individual passwords that are easier for them to remember. This will be accomplished as requested by our customers.

- 3.5 Direct the Security Officer to require the use of automated log-off feature for non-use.

MANAGEMENT AGREES - This feature is not currently available from the dial-in security vendor. All current City computer systems, except the Traffic Intertie system, already have an automated log-off feature that is being utilized. If the feature for the dial-in security system becomes available, OMS will evaluate its benefits and costs.